ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

An Efficient Way of Securing the Data in MANETS Using MRA Technique with RSA Algorithm

Mahesh K S[1], S Girish[2]

M.Tech Student, Department of Computer Science & Technology, Sahyadri College of Engineering and Technology , Mangaluru, India [1]

Asst. Prof., Department of Computer Science & Technology, Sahyadri College of Engineering and Technology , Mangaluru, India [2]

Abstract: Moving to wireless network from wired network has been a global trendy in the last few decades. The most important fact about wireless network is it's mobility. One of the most used and familiar applications of wireless networks is Mobile Ad hoc NETwork (MANET). MANET does not require any fixed network infrastructure; each node works as both a transmitter and receiver. Nodes imparts directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement new intrusion-detection systems to check malicious nodes in a network and which make the improved network performance.

Keywords: IDs, ACK, S-ACK, MRA, TWOACK, AACK.

I. INTRODUCTION

Because of natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the last few decades.

By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days [2]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.

In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [1], [4],. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery.[7] Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations [1], [5].Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance.

Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [1], attackers can

DOI 10.17148/IJARCCE.2016.5628

easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. BACKGROUND

As there are some limitations of MANET such as routing protocol, in routing protocol nodes always think that they are co-operative to each other to transfer data. This assumptions leave attackers to attack the nodes in MANET. IDS should be added in MANET for security level. Before this, let us discuss the approach used in MANET, namely, Watchdog.[3]
Watchdog – Watchdog is also an IDS for MANETs. Watchdog was designed for detecting malicious node misbehavior in the network. In Watchdog next hop transmission is used for detecting malicious nodes. Watchdog listens to its next hop transmission. If a Watchdog node overhears that its next node fails to forward the packet for a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as misbehaving. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping[6].

It is designed to overcome three of the six weaknesses of Watchdog approach, as, false misbehavior, limited transmission power, and receiver collision.

I. Receiver collision:

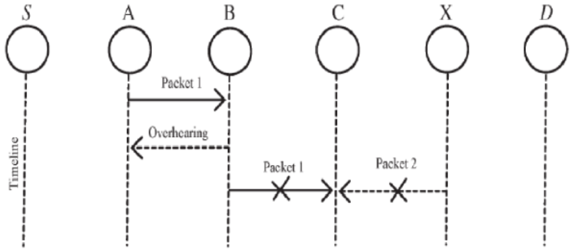


Figure 1 Receiver collision

In above figure, Node A sends Packet1 to Node B, and tries to overhear whether Node B has sent Packet1 to Node C, but meanwhile Node X sends Packet2 to Node C. In such case, Node A gets to know that Node B has forwarded the Packet 1 to Node C. But at Node C there is collision between two packets i.e. Packet1 and Packet2. So because of it, Node A fails to overhear that Node C has got the Packet1 or not.

II. Limited transmission power:
In below figure, Node B purposely limits its transmission power. So now Node A can hear that Node B has sent Packet1 to Node C. But as Node B has limited its transmission power Node A cannot hear whether Node C has received Packet1 or not.

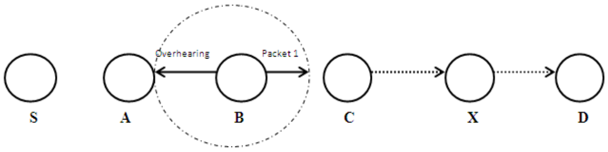


Figure 2. Limited transmission power

III. False misbehavior behavior:

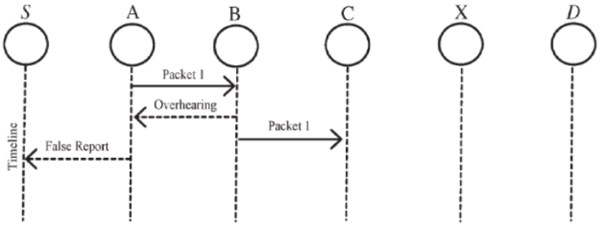


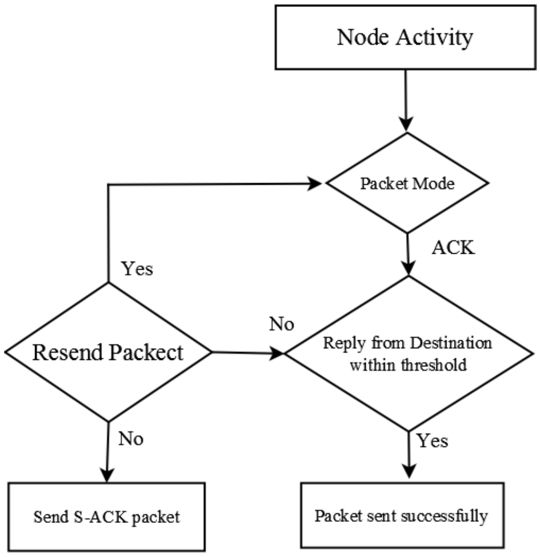
Figure 3. False misbehavior behavior

In above figure, Node A sends Packet1 to Node B. As Node B receives Packet1 it immediately sends Packet1 to Node C. Now Node A gets to know that Node B has successfully forwarded the packet to Node C, still Node A sends false report to the source node or previous node that Node B is misbehaving. This is known as false misbehavior report.

III.SYSTEM ARCHITECTURE

In this section we introduce a combination of different IDs which are used for MANETs, and Proposed system consists of three major methods, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

A. ACK:

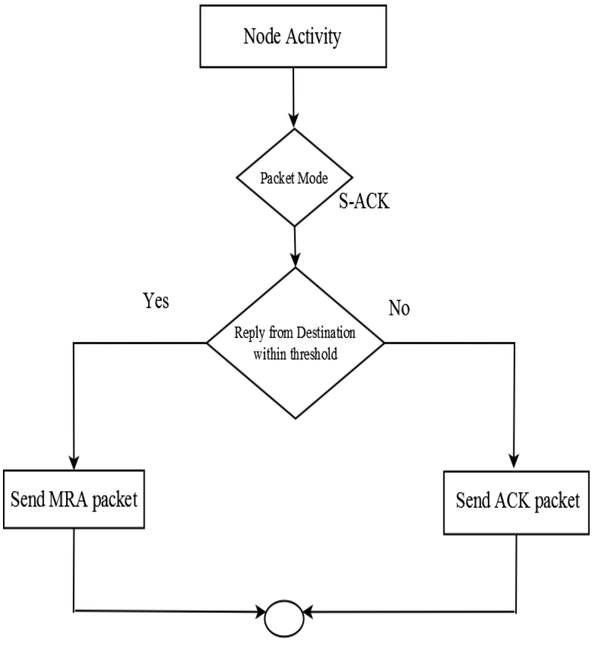


ACK

DOI 10.17148/IJARCCE.2016.5628

ACK is basically an end-to-end acknowledgment scheme. In this, first node has to send Packet to second node, and that second node has to give back acknowledgment to the first node. If within time period the second node doesn't send back acknowledgment then again that Packet is being send.

B. Secure ACK (S-ACK):
S-ACK is similar to TWOACK. In S-ACK three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node [3]. In TWOACK scheme, the source node immediately trusts the misbehavior report sent by the other intermediate nodes, there is a mode named MRA, which first confirm whether the node is misbehaving or not, and then takes the decision of declaring it malicious.



S-ACK

C. MRA:
MRA scheme is designed to resolve the weakness of Watchdog. Watchdog fails to detect the false misbehavior report.

When the source node gets the report of false misbehavior, at that time the source node sends the report to MRA mode. Then in the MRA mode, another route is assigned through its local base knowledge and the same packet is sent again to the destination, but through different route. When the packet reaches destination, MRA checks whether the packet is reached its destination or not through its local knowledge base. If destination has already received the same packet before, then MRA concludes that it is a false report and whichever node generated this report is marked malicious. But if, the packet has reached its destination for the first time then the misbehavior report is trusted and accepted. Due to this scheme that it is capable of detecting malicious nodes.

D. RSA:
This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder therefore protecting unauthorized users from having access to the information even if they are able to break into the system.

By the adoption of MRA scheme it is capable of detecting malicious nodes despite the existence of false misbehavior report and also provides an encryption for MANETs with RSA algorithm.

IV. PERFORMANCE EVALUATION

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics [13].

1) Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2) Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR),ACK, S-ACK, and MRA].

3) Throughput: Throughput defines the rate of production or the rate at which something can be processed.

4) Delay: This defines difference at which packets sent time and received time.

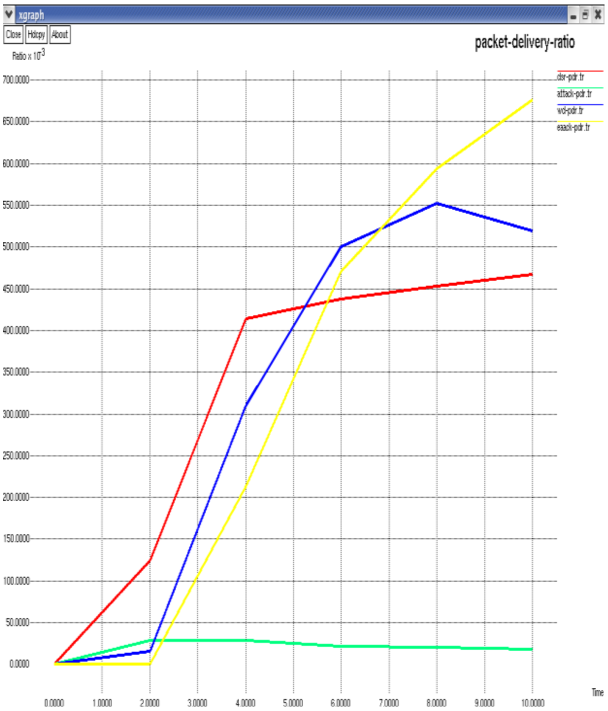


Figure 4: PDR Graph

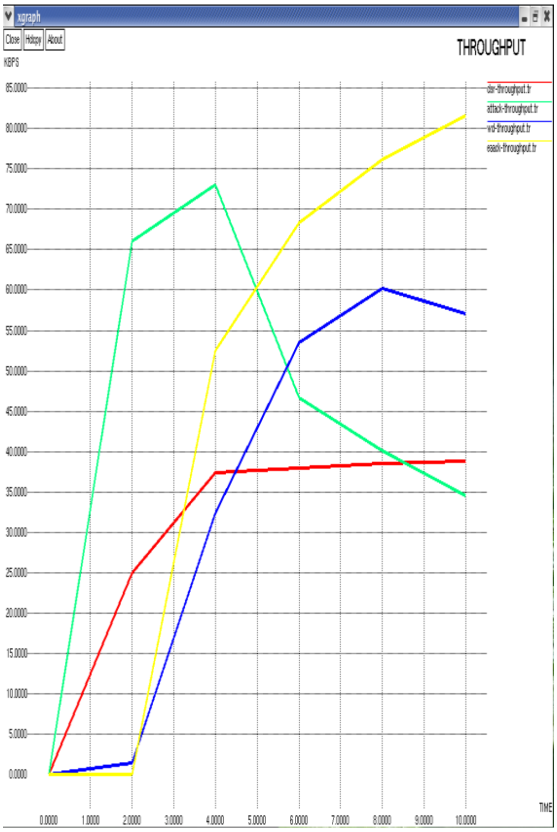


Figure 5: Throughput Graph

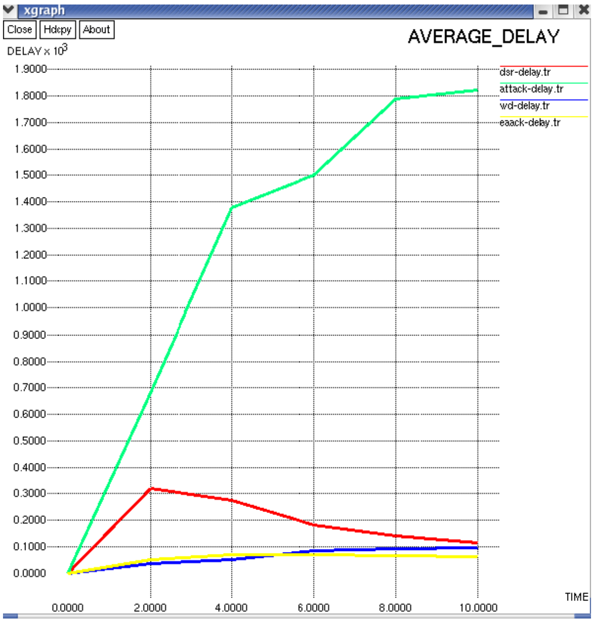


Figure 6: Delay Graph

V. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named MRA specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate with encryption with AES algorithm in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal AES in MANETs, we implemented both AES scheme in our simulation. Eventually, we arrived to the conclusion that the AES scheme is more suitable to be implemented in MANETs.

REFERENCES

[1] Sarika Patil., Bharat Tidke., "DH-EAACK Secure Intrusion Detection System to detect Black Hole Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.4, October 2014.

[2] Elhadi M. Shakshuki, Nang Kang, and Tarek R. Sheltami, "EAACK-A Secure intrusion-Detection System for MANETs," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[3] Poonam Joshi, Pooja Nande, Ashwini Pawar, Pooja Shinde, Rupali Umbare, "EAACK - A Secure Intrision and Prevention System for MANETs", International Conference on Pervasive Computing (ICPC).

[4] K.Chinthanai chelvan, T.Sangeetha, V.Prabakaran, D.Saravanan,"EAACK - A Secure Intrusion Detection System for MANET", IJIRCCE vol. 2,Issue 4, April 2014.

[5] M A Matin, Md. Monir Hossain, Md Foizul Islam, Muhammad Nazrul Islam, M Mofazzal HossainM."Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN".

[6] Milana N, Ramesh B, Gururaj H L, "Design and Implementation of node misbehavior in MANETs."IEEE Transactions.

[7] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior i MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 5, MAY 2007.

DOI 10.17148/IJARCCE.2016.5628